



Department of Economic Security
Information Technology Standards

Title: 1-38-0073 Session Control Standard

Subject: This policy defines required session controls for DES systems.

Effective Date:

03/07/05

Revision:

1

1. Summary of Policy Changes

1.1. Original Implementation

2. Purpose

The purpose of this standard is to coordinate DES efforts to prevent unauthorized access to critical systems via workstations left unattended. Unattended workstations logged into networks, systems, and applications may allow unauthorized access to confidential information and resources.

3. Scope

This policy applies to all DES administrative entities, councils, divisions, administrations, programs and non-DES entities.

4. Responsibilities

4.1. The DES Director, Deputy Directors, Associate Director, and Assistant Directors are responsible for implementing and enforcing this policy.

4.2. The DES CIO and the DES Division of Technology Services is responsible for implementing this policy.

4.3. DES divisions and programs are responsible for implementing this policy and monitoring compliance for the users and systems that they implement or sponsor.

5. Definitions and Abbreviations

5.1. Abbreviations

5.1.1. **AHCCCS** – Arizona Health Care Cost Containment System

5.1.2. **CIO** – Chief Information Officer

5.1.3. **CISO** – Chief Information Security Officer

5.1.4. **DTS** – Division of Technology Services

5.1.5. **DES** – Department of Economic Security

5.1.6. **GITA** – Government Information Technology Agency

5.1.7. **IT** – Information Technology

5.1.8. **ISA** – Information Security Administration

6. STANDARD

The following session controls provide minimum requirements for preventing unauthorized access to information, systems, applications, and networks via unattended workstations, regardless of location, throughout the State. Requirements shall be documented and maintained as part of, and in accordance with, GITA Statewide Standard P800-S810, Account Management.

6.1 Session/System Timeout:

A 30 minute timeout policy shall be placed on multi-user information systems and remote communication systems.

All system users must log off or lock their screen when going to meetings, lunch and at the end of the business day, regardless of the sensitivity of information on the system. Any exceptions must be documented.

Locking screensavers shall be in use on all personal computers (including laptops). Screensavers must be automatically activated by the personal computer's operating system after fifteen minutes of inactivity.

6.1.1 Password Protection for Locking Screens:

Requirements for password strength used on locking screen savers shall be determined by the capabilities of the applicable operating system. Passwords used to unlock screens must meet requirements of GITA Statewide Standard P800-S820, Authentication and Directory Services, unless otherwise prevented by the capabilities of the applicable operating system.

6.2. Access Logs: Access logs, shall be turned on and protected from accidental or deliberate overwriting. Systems should be configured to log information locally, and the logs should be sent to a remote system. Logs should contain details of:

- Access by types of user;
- Servicing activities;
- Failed sign-on attempts;
- Error / exception conditions; and
- Sufficient information to identify individual userIDs, resources, and information accessed, access paths, and patterns of access.
- Access logs shall be maintained for a period of 180 days.

7. Implications

DES business units must review their existing rules and processes and educate their employees and stakeholders.

8. Implementation Strategy

This standard is effective for all DES business units as of its publication.

9. References

9.1. None

10. Attachments

10.1. None

11. Associated GITA IT Standards or Policies

11.1. P800-S810 GITA Statewide Standard, Account Management

12. Review Date

12.1. This document will be reviewed twelve (12) months from the original adoption date, and every twelve months thereafter.